

ABSTRACT

Data are converted between an unencrypted and an encrypted format according to the Rijndael algorithm, including a plurality of rounds. Each round is
5 comprised of fixed set of transformations applied to a two-dimensional array, designated state, of rows and columns of bit words. At least a part of said transformations are applied on a transposed version of the state, wherein rows and columns are transposed for
10 the columns and rows, respectively.

(Figure 6)

FIG. 6
is a diagram illustrating the state of the Rijndael algorithm, showing the state as a 4x4 array of bytes, with the state being transposed for the columns and rows, respectively.